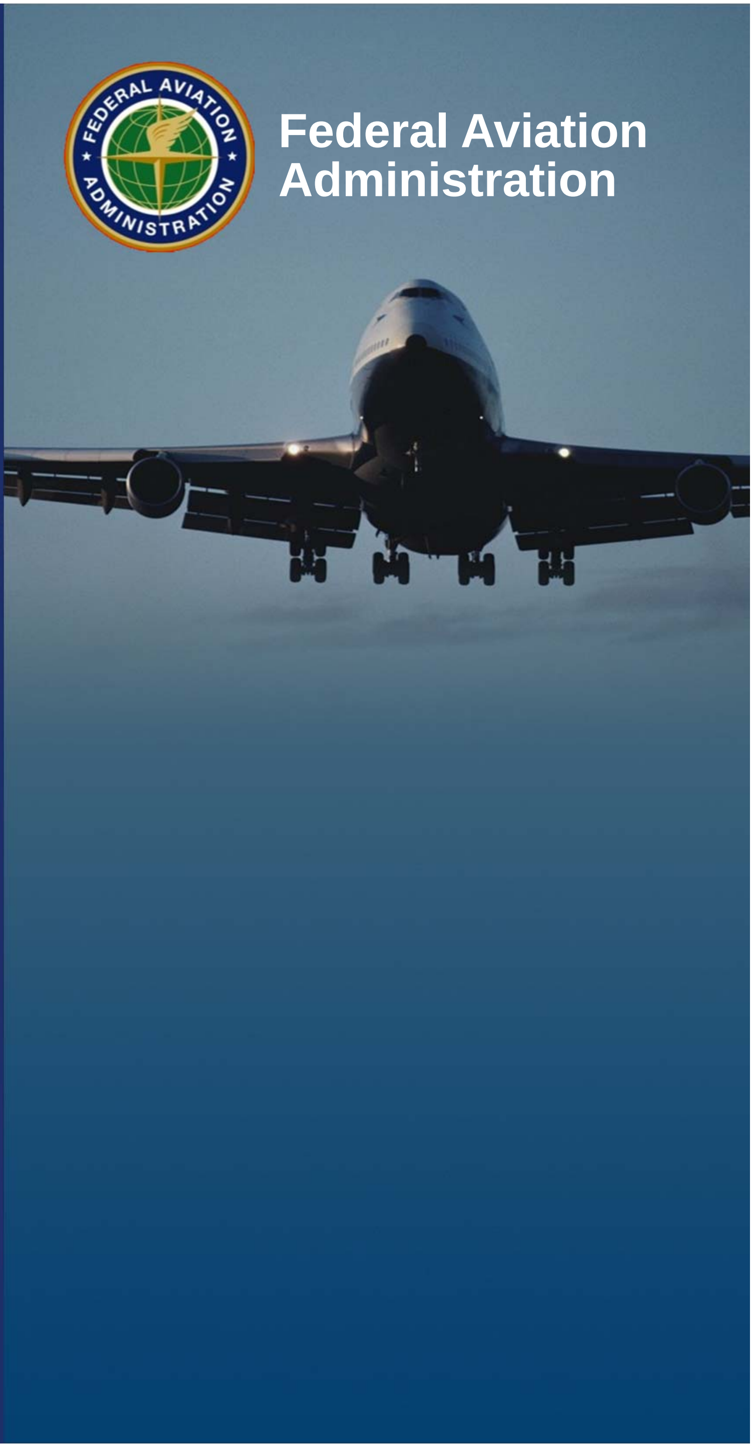
ICAO Air-Ground Security Standards Strategy

Presenter: Vic Patel

Date: April 19 2012



Federal Aviation Administration

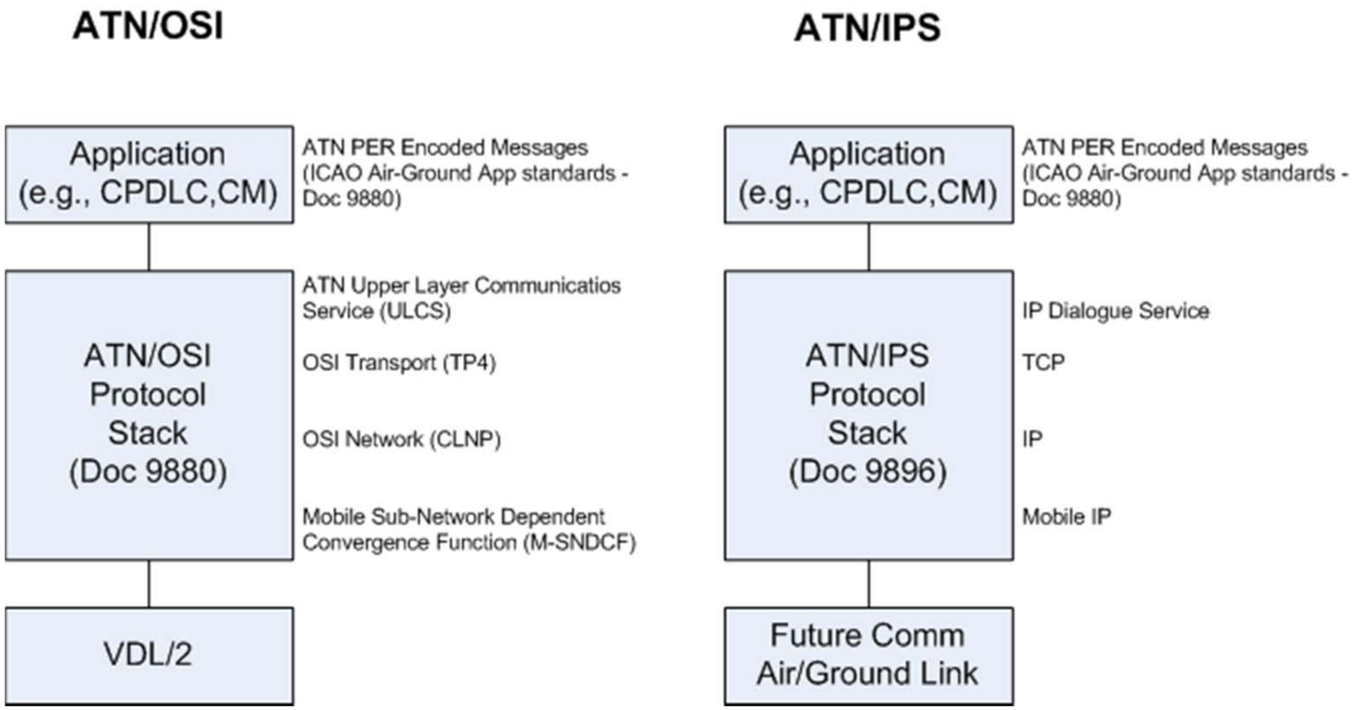
Agenda

- Goals and objectives
- Background (ATN/OSI and ATN/IPS)
- ATN/OSI Protocol Stack
- Original Security addition to OSI Protocol Stack
- Simplification of Security in ATN/OSI Protocol Stack – Secure Dialogue Service
- Use of Secure Dialogue Service in ATN/IPS Protocol Stack
- Summary for ATN/OSI Approach
- Doc 9880 Changes
- Application Public Keys Provided by Secure Dialogue Sevice (instead of CM)

Air-Ground security goals

- Security strategy for air/ground link – ATN
- Complete ICAO standards
- Work with industry and standards community – Airlines, Service providers, ICAO, RTCA, EURCAE, AEEC, EUROCONTROL, IETF
- Global harmonization: transition to ATN, security, and NextGen/SESAR

ATN/OSI & ATN/IPS Protocol Stack



ATN/OSI

Application (e.g., CPDLC,CM)

ATN PER Encoded Messages (ICAO Air-Ground App standards - Doc 9880)

ATN/OSI Protocol Stack (Doc 9880)

ATN Upper Layer Communicatios Service (ULCS)

OSI Transport (TP4)

OSI Network (CLNP)

Mobile Sub-Network Dependent Convergence Function (M-SNDCF)

VDL/2

ATN/IPS

Application (e.g., CPDLC,CM)

ATN PER Encoded Messages (ICAO Air-Ground App standards - Doc 9880)

ATN/IPS Protocol Stack (Doc 9896)

IP Dialogue Service

TCP

IP

Mobile IP

Future Comm Air/Ground Link

- ICAO has specified two protocol stacks
- The ATN/OSI applications and protocol stack is specified in Doc 9880.
- The ATN/IPS protocol stack is specified in Doc 9896.
  - Doc 9896 defines the IP Dialogue Service which permits legacy (ATN/OSI) applications to operate over the new IPS protocol stack.

ATN/OSI Protocol Stack

The ATN/OSI stack consists of:

- The Upper Layer Communications Service (ULCS) presents a common logical interface to the applications called the Dialogue Service.
- ULCS's primary function is to establish a session among communicating peers on the airborne and ground sides. The ULCS contains a streamlined version of the OSI Presentation and Session Layers.
- ULCS runs over the OSI defined class 4 transport protocol (TP4). TP4 in turn runs over the OSI network layer using the CLNP protocol.
- In the air-ground environment CLNP operates over the Mobile Sub-Network Dependent Convergence Function (M-SNDCF). The M-SNDCF runs over VHF Data Link Mode 2 (VDL/2).

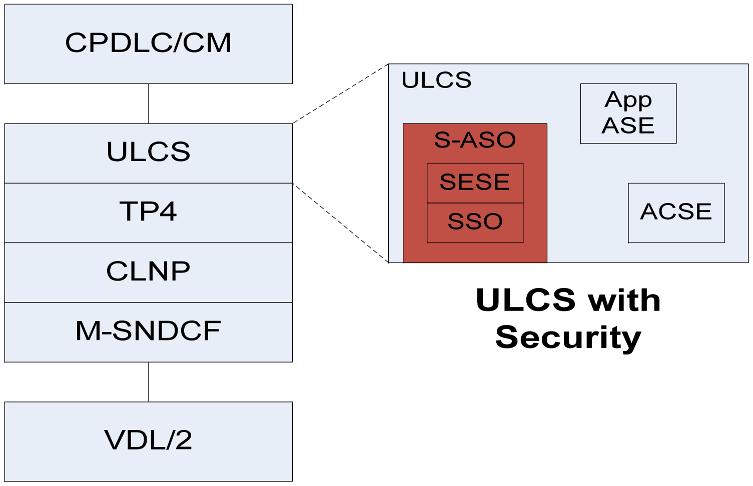
ATN/IPS Protocol Stack

The ATN/IPS stack consists of:

- The IP Dialogue Service which presents the same logical interface to the legacy ATN applications as the Dialogue Service.
- The IP Dialogue Service provides the ULCS Dialogue Service primitives and carries the Dialogue Service parameters to the peer application.
- The IP Dialogue Service runs over the IETF TCP protocol. TCP in turn runs over the network layer using the IP protocol.
- In the air-ground environment IP operates using the IETF Mobile IP protocol. Mobile IP is anticipated for use over Future Comm Air-Ground subnetworks.

Original Security approach to ATN/OSI Protocol Stack

ICAO Doc 9705 ATN/OSI



ULCS with Security

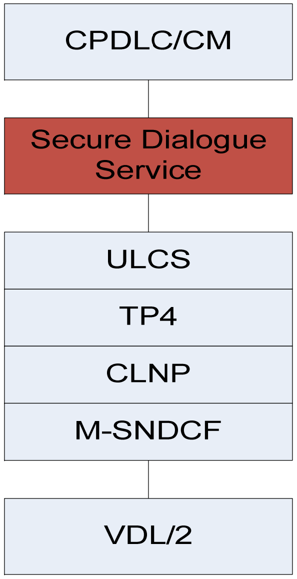
- The standards for securing air-ground communications were developed in ICAO communications panels as an extension to the OSI standards. Figure depicts the addition to the ATN/OSI protocol stack as specified in Doc 9705 Edition 3.

- Edition 3 of Doc 9705 placed the Security Application Service Object (S-ASO) in the ULCS. The S-ASO uses the OSI-defined Security Exchange Service Element (SESE) and invokes the ATN-defined Security Service Object (SSO), which performs the cryptographic functions.

- ULCS security approach is fairly complex and difficult to implement

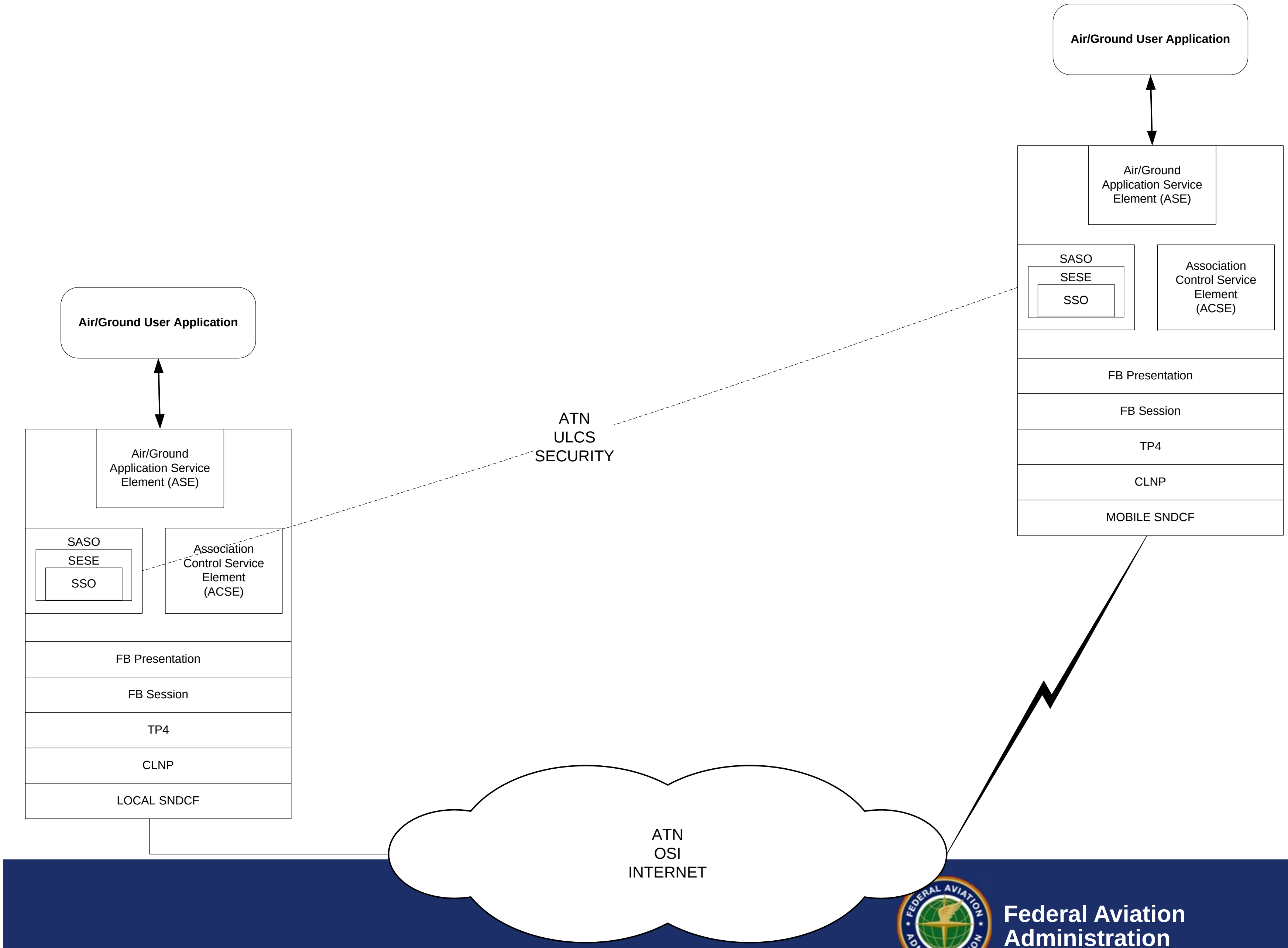
Proposal to Simplify Security in ATN/OSI Protocol Stack – Secure Dialogue Service

ICAO Doc 9880 ATN/OSI with Secure Dialogue Service



- Proposal for (Doc 9880) ATN/OSI Protocol Stack with Security
- The Edition 3 placement of security in the ULCS is considered to involve significant complexity. It would require a completely new implementation of the current ULCS. In order to simplify implementation of ATN Security, the FAA has been coordinating with EUROCONTROL to define an alternative implementation that would be simpler to implement and not require changes to the ULCS. This alternative implementation is called the Secure Dialogue Service.
- The figure shows the insertion of the Secure Dialogue Service as a sub-layer between the applications and the ULCS.
- Note that the Secure Dialogue Service still implements the Security Service Object (SSO) to perform the cryptographic functions. However it eliminates the complexity of doing security in the ULCS using the S-ASO and SESE.

ICAO DOC 9705 edition 3 ATN ULCS Security Implementation



Air/Ground User Application

Air/Ground Application Service Element (ASE)

SASO

SESE

SSO

Association Control Service Element (ACSE)

FB Presentation

FB Session

TP4

CLNP

LOCAL SNDCF

ATN ULCS SECURITY

Air/Ground User Application

Air/Ground Application Service Element (ASE)

SASO

SESE

SSO

Association Control Service Element (ACSE)

FB Presentation

FB Session

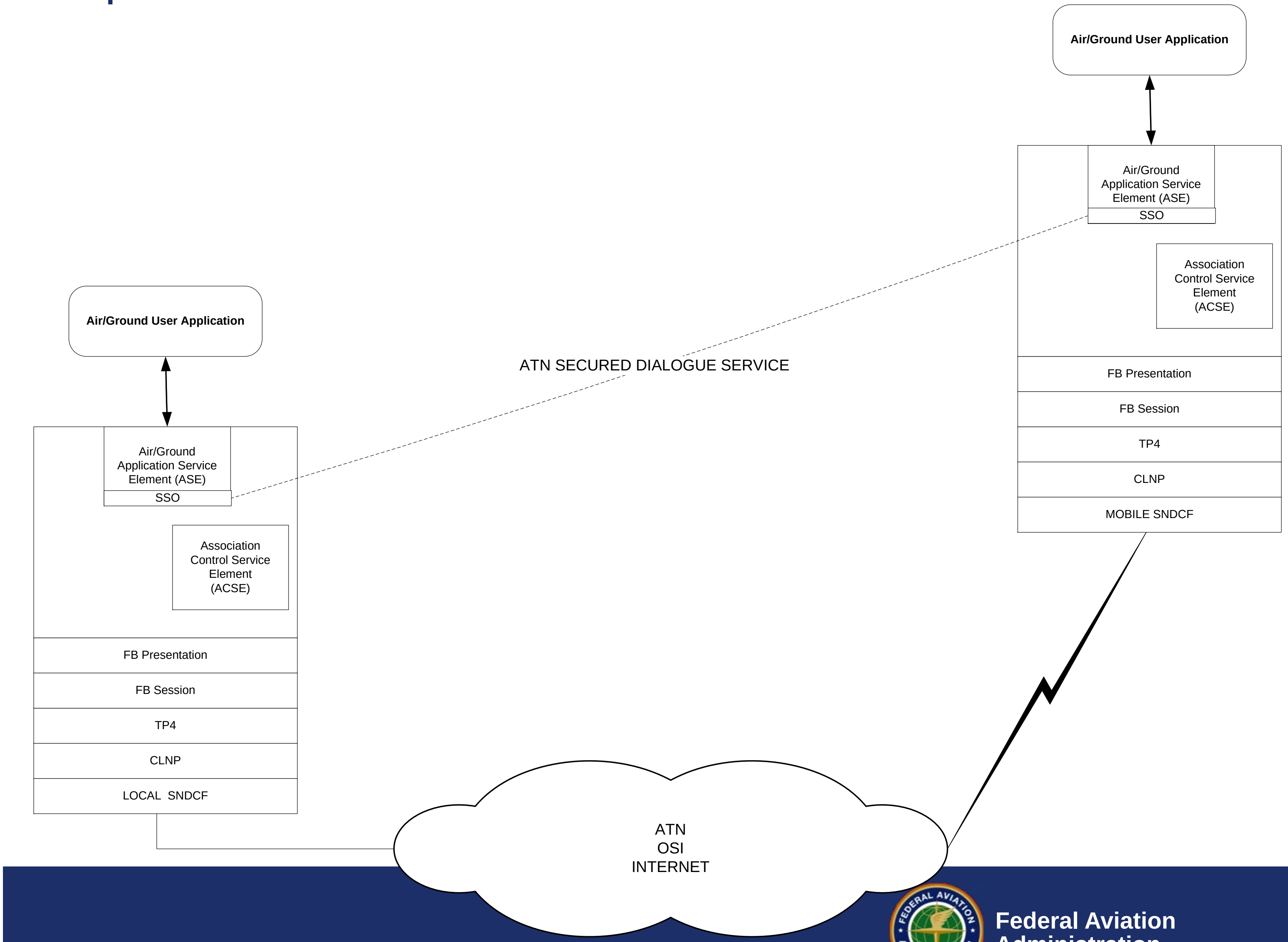
TP4

CLNP

MOBILE SNDCF

ATN OSI INTERNET

Proposed ICAO Doc 9880 ATN SECURED DIAOGUE SERVICE OVER ATN OSI



Air/Ground User Application

Air/Ground Application Service Element (ASE)

SSO

Association Control Service Element (ACSE)

FB Presentation

FB Session

TP4

CLNP

LOCAL SNDCF

ATN SECURED DIALOGUE SERVICE

Air/Ground User Application

Air/Ground Application Service Element (ASE)

SSO

Association Control Service Element (ACSE)

FB Presentation

FB Session

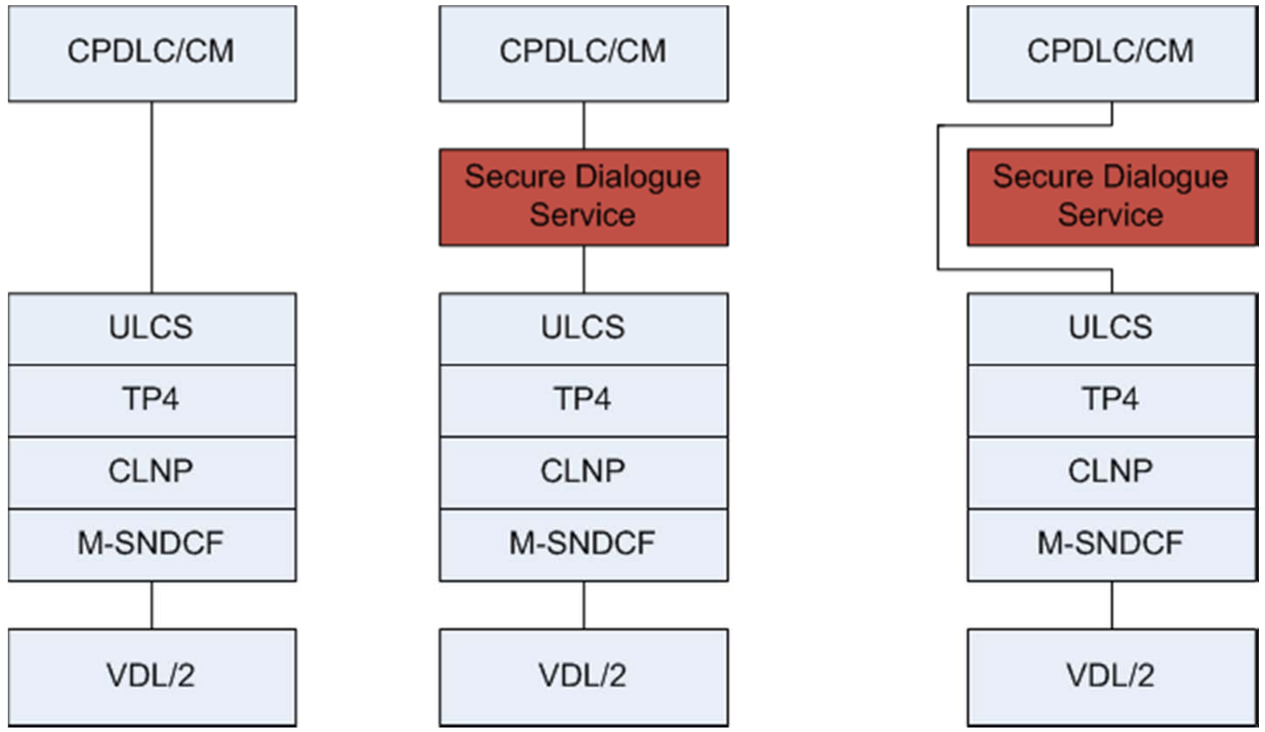
TP4

CLNP

MOBILE SNDCF

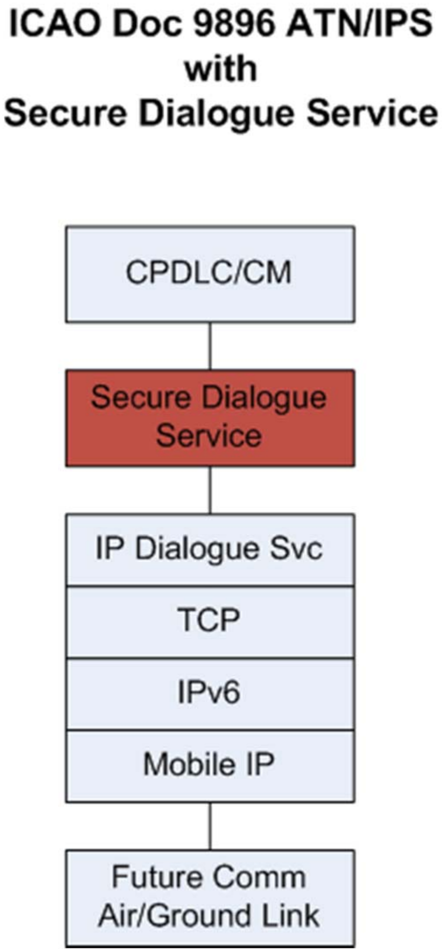
ATN
OSI
INTERNET

Implementation Options for Secure Dialogue Service



- The proposal for the Secure Dialogue Service permits implementation options depending on the operational domain
  - If security is not used in a particular domain the Secure Dialogue Service may not be implemented
  - The Secure Dialogue service could be implemented but its use or not would depend on the operational domain
- The Applications and ULCS would be implemented the same whether or not the Secure Dialogue Service is implemented or used.

Proposal to Use of Secure Dialogue Service in ATN/IPS Protocol Stack



- ICAO has defined a new version of the ATN which uses the Internet Protocol Suite (IPS). This stack has been defined in ICAO Doc 9896.
- It uses the well-known TCP/IP protocols and Mobile IP as the mobility solution.
- Doc 9896 includes an IP Dialogue Service which allows legacy (ATN/OSI) applications such as CPDLC and CM to operate in the ATN/IPS environment.
- The IP Dialogue Service presents the same logical interface to legacy applications as in the OSI environment.

- Figure shows the use of the Secure Dialogue Service in the ATN/IPS environment. In addition to the benefits of simplification described above the result is that there would be one ATN Security implementation that could be used in both the ATN/OSI and ATN/IPS environments.

Summary for Secure Dialogue Service Approach

- The original Doc 9705 Edition 3 approach to ATN Security is a validated standard. It has the disadvantage that its implementation in the ULCS introduces significant complexity to the ULCS and requires that the complete ULCS be replaced.

- The proposed Secure Dialogue Service approach would simplify the implementation of ATN Security
  - Security is all performed in the same place, i.e., in the Secure Dialogue Service sub-layer

- The Doc 9880 ULCS can be updated to remove the security features. This will become a equivalent to Doc 9705 Edition 2 but with PDRs incorporated

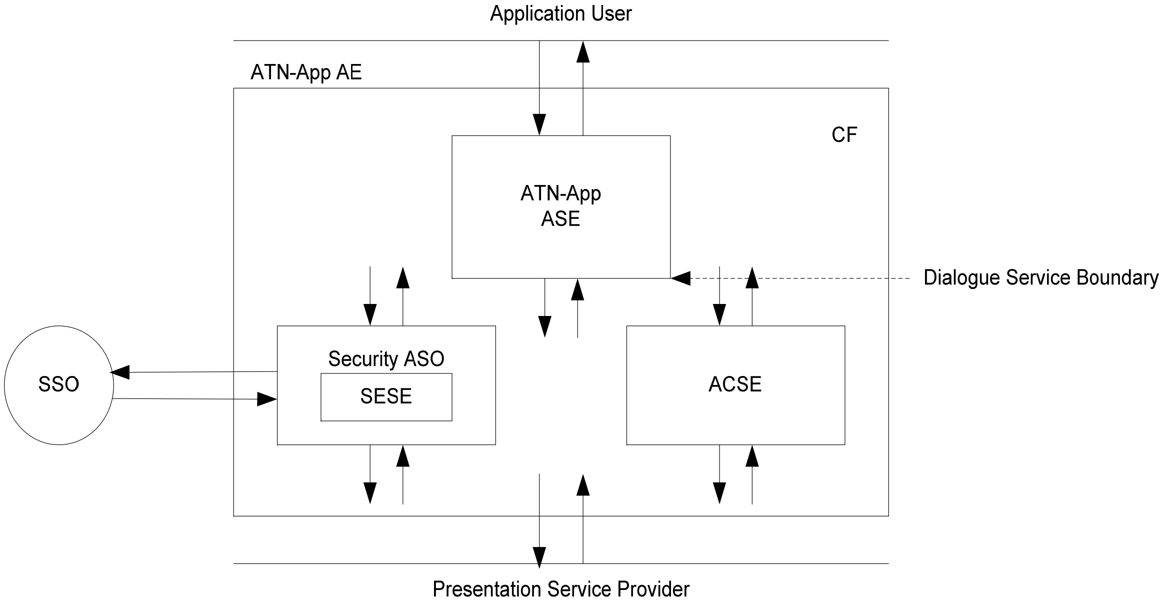
- The Secure Dialogue Service provides implementation options:
  - It can not be implemented or implemented and used or not depending or the operational domain
  - In any case the applications and ULCS would be the same

- The Secure Dialogue Service has the added advantage that it can be used in the ATN/IPS stack.

Doc 9880 Changes

- Security in the ULCS
- Security using the Secure Dialogue Service
- Changes to Doc 9880 ULCS
- Proposal for Secure Dialogue Service in to Doc 9880 Security

Security in the ULCS

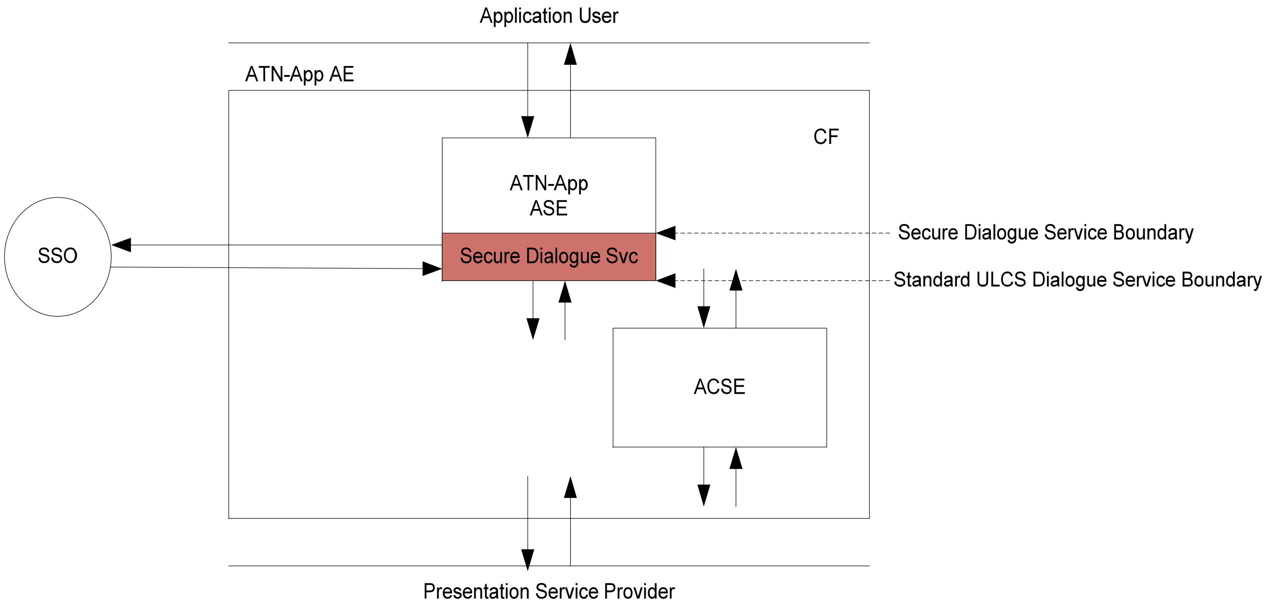


- Security in the ULCS requires insertion of the Security ASO and SESE, modification of ACSE and more significantly modification of the Control Function.

•The "outer" dialogue service CF controls the interactions between the Application ASE (e.g. CPDLC air or ground ASE), the Security ASO, ACSE and the supporting transport service.

•The Security ASO itself contains an "inner" CF, which controls the interactions between the S-ASO upper and lower service boundaries, the embedded SESE upper and lower service boundaries, and the SSO.

Security using the Secure Dialogue Service


Application User
ATN-App AE
CF
ATN-App ASE
SSO
Secure Dialogue Svc
Secure Dialogue Service Boundary
Standard ULCS Dialogue Service Boundary
ACSE
Presentation Service Provider

- Security with the Secure Dialogue Service removes:

  •the S-ASO,

  •SESE,

  •the enhanced ACSE, and the

  •logic of the ULCS Control Function,

•The same SSO primitives are invoked directly by Secure Dialogue Service primitives.

Changes to Doc 9880 ULCS

- The PDR changes not related to security must be left in Doc 9880.
- The major changes are to:
  - Modify the overall architecture to remove the Security ASO and SESE.
  - Change the Control Function essentially back to the equivalent of Doc 9705 Edition 2.
  - Remove the enhanced ACSE features.
  - Remove the Security ASO
  - Remove the SESE
  - Modify the ASN.1 structures to remove the security exchange items imported from the OSI security framework.

Proposal for Changes to Doc 9880 Security

- Incorporate proposed PDR changes not related to the Secure Dialogue Service.
- For the Secure Dialogue Service a new section must be inserted which specifies the Secure Dialogue Service Primitives:
    - sD-START Request primitive
    - sD-START Indication primitive
    - sD-START Response primitive
    - sD-START Confirmation primitive

    - sD-DATA Request primitive
    - sD-DATA Indication primitive

    - sD-END Request primitive
    - sD-END Indication primitive
    - sD-END Response primitive
    - sD-END Confirmation primitive

    - sD-ABORT Request primitive
    - sD-ABORT Indication primitive
    - sD-P-ABORT Indication primitive
  - These primitives incorporate the logic of the Control Function and Security ASO to invoke the SSO.
- New ASN.1 structures must be introduced to carry the information that had been carried in the ULCS security exchange items

Application Public Keys Provided by Secure Dialogue Service

- Application Public Keys Provided by CM
- Key Establishment CM and ULCS
- Key Establishment CM and SDS

Application Public Keys Provided by CM

- In current Doc 9880 ULCS and CM and draft Security Part, public keys for ground applications are returned in the CM Logon Response message.

- This approach distributes security across the ULCS and the CM application.

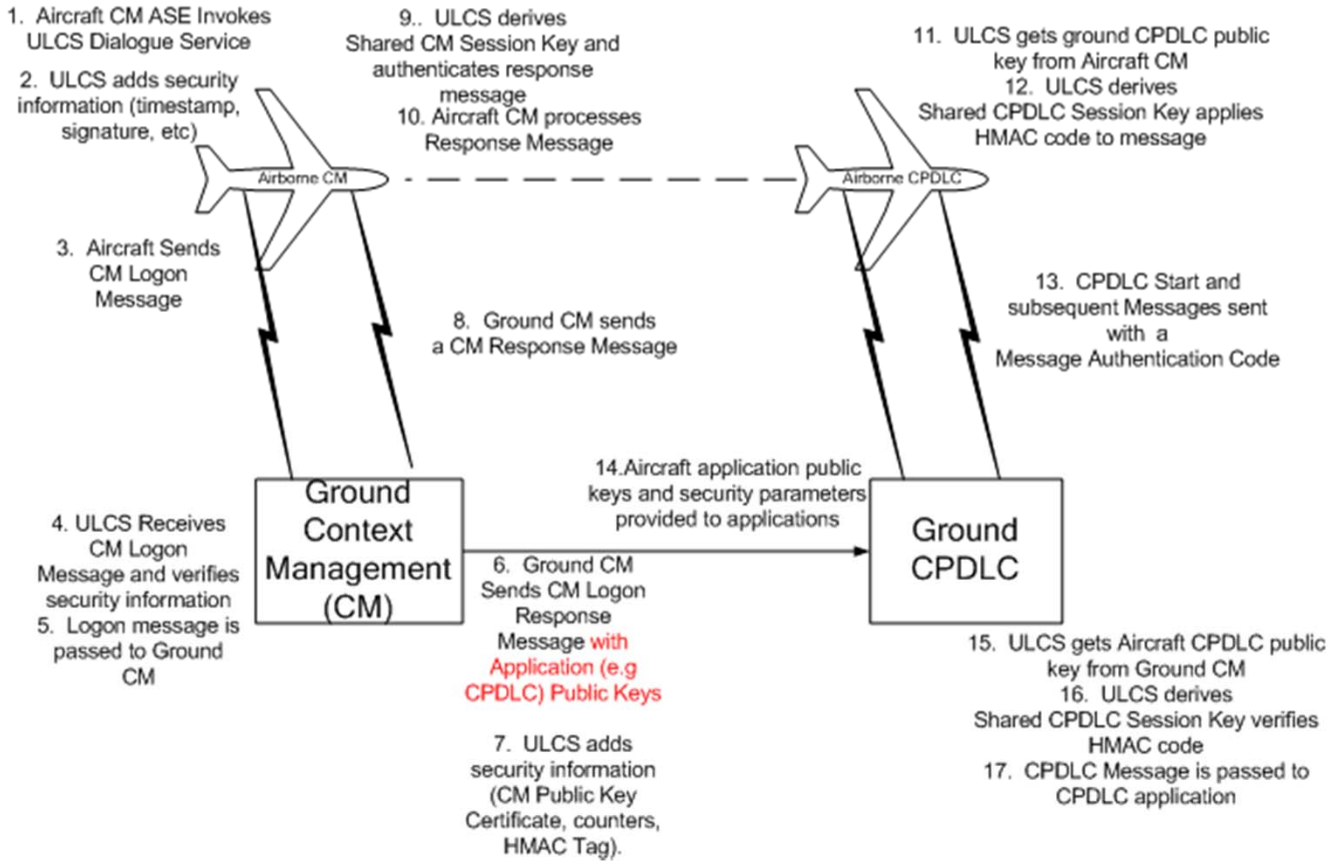
- The aircraft ULCS security function in particular must get the public key of the application (for example CPDLC’s public key) from the aircraft CM application.

- All other security parameters are retrieved from information exchanged within the security parts of the ULCS.

- Under the Secure Dialogue Service it would be possible to have the application public keys sent along with other security information within the Secure Dialogue Service

- This would require implementing this in the Secure Dialogue Service and removing it from the Doc 9880 CM
  - The changes are mainly to remove this from the ASN.1 message definitions

Key Establishment CM and ULCS



1. Aircraft CM ASE Invokes ULCS Dialogue Service

2. ULCS adds security information (timestamp, signature, etc)

3. Aircraft Sends CM Logon Message

4. ULCS Receives CM Logon Message and verifies security information

5. Logon message is passed to Ground CM

6. Ground CM Sends CM Logon Response Message with Application (e.g CPDLC) Public Keys

7. ULCS adds security information (CM Public Key Certificate, counters, HMAC Tag).

8. Ground CM sends a CM Response Message

9.. ULCS derives Shared CM Session Key and authenticates response message

10. Aircraft CM processes Response Message

11. ULCS gets ground CPDLC public key from Aircraft CM

12. ULCS derives Shared CPDLC Session Key applies HMAC code to message

13. CPDLC Start and subsequent Messages sent with a Message Authentication Code

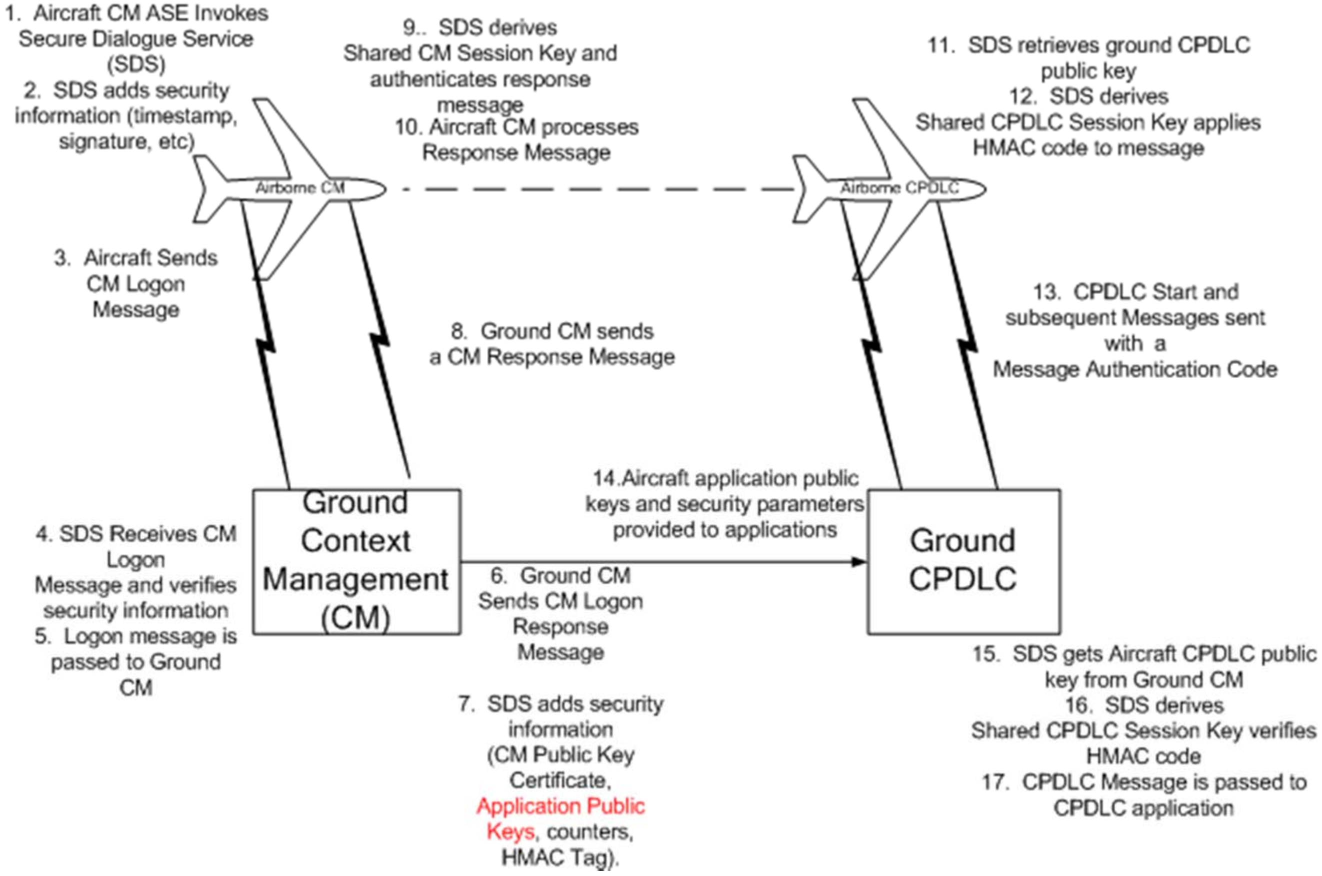
14.Aircraft application public keys and security parameters provided to applications

15. ULCS gets Aircraft CPDLC public key from Ground CM

16. ULCS derives Shared CPDLC Session Key verifies HMAC code

17. CPDLC Message is passed to CPDLC application

Key Establishment CM and SDS



1. Aircraft CM ASE Invokes Secure Dialogue Service (SDS)
2. SDS adds security information (timestamp, signature, etc)

9.. SDS derives Shared CM Session Key and authenticates response message
10. Aircraft CM processes Response Message

11. SDS retrieves ground CPDLC public key
12. SDS derives Shared CPDLC Session Key applies HMAC code to message

3. Aircraft Sends CM Logon Message

8. Ground CM sends a CM Response Message

13. CPDLC Start and subsequent Messages sent with a Message Authentication Code

14.Aircraft application public keys and security parameters provided to applications

4. SDS Receives CM Logon Message and verifies security information
5. Logon message is passed to Ground CM

6. Ground CM Sends CM Logon Response Message

7. SDS adds security information (CM Public Key Certificate, Application Public Keys, counters, HMAC Tag).

15. SDS gets Aircraft CPDLC public key from Ground CM
16. SDS derives Shared CPDLC Session Key verifies HMAC code
17. CPDLC Message is passed to CPDLC application